REMARKS

Applicants thank the Examiner for the careful and thorough examination of the present application. The patentability of the claims is discussed in detail below.

I. The Invention

The invention is directed to a cryptographic device. Independent Claim 1, for example recites a cryptographic device which includes a cryptographic module and a communications module coupled thereto. More particularly, the cryptographic module includes a user network interface, a host network processor coupled to the user network interface, and a cryptographic processor coupled to the host network processor. Additionally, the communications module includes a network communications interface coupled to the cryptographic processor. The host network processor generates cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and it also encapsulates command packets for the communications module interface in the data portions of the cryptographic processor command packets. Moreover, the cryptographic processor passes the command packets to the communications module without performing cryptographic processing thereon.

Independent Claim 12 is directed to a cryptographic device as recited in independent Claim 1 further reciting the user network interface as a LAN interface, the command packets as Ethernet command packets, and the host network processor formatting the data portions based upon the simple network

management protocol. Independent Claim 21 is a method counterpart to independent Claim 1. Independent Claim 26 is a system counterpart to independent Claim 1 further reciting the host network processor formatting the data portions based upon the simple network management protocol.

II. The Claims are Patentable

The Examiner rejected independent Claims 1 and 21 over a combination of Dellmo et al. (U.S. Patent Publication No. 2002/0095594), assigned to the assignee of the current application, and Stallings (Cryptography and Network Security: Principles and Practice). Independent Claims 12 and 26 were rejected further in view of Stevens.

Dellmo et al. is directed to a secure wireless LAN device including a housing, a wireless transceiver carried by the housing, and a cryptography circuit carried by the housing. A media access controller (MAC) is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface carried by the housing and connected to the MAC.

The Examiner correctly recognized that Dellmo et al. does not disclose the host network processor generating cryptographic processor command packets for the cryptographic processor each having an address portion and a data portion, and encapsulating command packets for the communications

module interface in the data portions of the cryptographic processor command packets.

Moreover, the Examiner also correctly recognized that Dellmo et al. does not disclose the cryptographic processor passing the command packets to the communications module without performing cryptcgraphic processing thereon. The Examiner then turned to Stallings for these noted critical deficiencies of the primary reference, Dellmo et al. Stallings is a general cryptography textbook, and the Examiner pointed particularly to the text on page 418, lines 8-13, which discloses encrypting IP packets for transmission through an Internet firewall:

> The source prepares an inner IP packet with a destination address of the target internal host. This packet is prefixed by an ESP header; then the packet and ESP trailer are encrypted and Authentication Data may be added. The resulting block is encapsulated with a new IP header (base header plus optional extensions such as routing and hop-by-hop options for Ipv6) whose destination address is the firewall; this forms the outer IP packet. (Emphasis added).

The Examiner contended that Stallings discloses the cryptographic processor passing the communications module command packets to the communications module without performing cryptographic processing thereon, as in the claimed invention. Applicants submit that the Examiner mischaracterized Stallings, as it does not pass the communications module command packets (inner packets), which are encapsulated in the data portions of the cryptographic process command packets, to the communications module without

performing cryptographic processing thereon. Instead, Stallings discloses the inner packet and ESP trailer being encrypted prior to the encapsulation and passing of the command packet, as illustrated in the cited passage above. Accordingly, even a selective combination of Dellmo et al. and Stallings fails to disclose the claimed invention.

Additionally, as previously noted, Dellmo et al. is directed to a secure wireless LAN device. A MAC is included and implements a predetermined wireless LAN MAC protocol. The cryptography circuit includes a cryptography processor, and a control gateway circuit connected to the MAC and the wireless transceiver. The secure wireless LAN device also includes a user network interface connected to the MAC. In contrast, Stallings, although a general text, is directed to the case where an external host wishes to communicate with a host on an internal network protected by a firewall, and which ESP is implemented in the external host and firewalls (page 418, lines 3-5). A person having ordinary skill in the art would not turn to the ESP implemented network/firewall technology disclosed in Stallings to generate, process, and pass packets from the internal processors and modules on an ESP independent cryptographic device in Dellmo et al. Accordingly, the combination of Dellmo et al. and Stallings is improper.

Moreover, in Stallings, the resulting packet is encapsulated with a new IP header and has a destination address of the firewall (page 418, lines 11-13). Implementing Stallings into Dellmo et al. would destroy the functionality of Dellmo et al. since the packets are generated for passing

between the cryptographic processor and the communications module internal to the device.

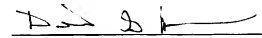
The Examiner also rejected independent Claims 12 and 26 over a three-way combination of Dellmo et al., Stallings, and Stevens. Stevens is cited as disclosing an SNMP protocol. Stevens adds nothing to the critical deficiencies of Dellmo et al. and Stallings.

Accordingly, it is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

III. Conclusion

In view of the arguments presented above, it is submitted that all of the claims are patentable. Accordingly, a Notice of Allowance is respectfully requested in due course. If the Examiner determines any remaining informalities exist, he is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicants